foto: Jihočeská univerzita v Českých Budějovicích

Jihočeská univerzita: Efektivní správa identit s Wren:IDM

70 000 identit (15 000 aktivních)

5 zdrojových systémů

- systém pro studijní agendu IS/STAG
- personální systém EGJE
- systém pro celoživotní vzdělávání
- karetní systém
- evidence budov a místností

8 řízených systémů

- Active Directory
- LDAP
- Aleph
- DB
- RADIUS LDAP
- ...

reference

> IdM nasazený firmou Orchitech si nás získal svojí rychlostí a spolehlivostí. Dle systému RT teď řešíme o 80 % méně požadavků. Zbylých 20 % pak tvoří převážně jen zapomenutá hesla. Řešení pokrylo všechny naše potřeby, a to ve slíbeném termínu.

Ing. Jan Marek

Vedoucí Útvaru správy informační infrastruktury Jihočeské univerzity

výzva

Když staré řešení nestačí

Původní IdM od společnosti Novell přestalo Jihočeské Univerzitě (JU) vyhovovat.
Implementace procesů zastarala, byla chybová a jakkoliv upravit konfiguraci bylo složité. „V původní implementaci bylo v podstatě nemožné provést rekonciliaci, tj. srovnání chtěného a aktuálního stavu systému, který se z nějakého důvodu rozsynchronizoval," uvádí k původnímu stavu pan Marek.
Dále došlo ke změně cenové politiky výrobce původního systému s naceněním dle počtu identit. Těch má univerzita desítky tisíc, čímž se licence neúměrně a neudržitelně prodražily. Univerzita tak musela přistoupit ke změně systému.

Tím se otevřelo okno příležitosti k implementaci procesů dle aktuálních potřeb a řadě vylepšení. „Univerzita dopředu tušila, že bude lepší přejít na nový systém. Hlavním parametrem pro výběr nového systému přitom bylo TCO, tedy snížení nákladů oproti původnímu řešení," říká pan Marek.
Orchitech zvítězil ve výběrovém řízení a dodal řešení postavené na produktu Wren:IDM, open-source nástupci projektu OpenIDM. „Získali jsme zcela nový systém, který je spolehlivější, rychlejší, predikovatelnější a v případě havárií lze stav jednoduše narovnat, ať už na vstupu do IdM, kdy si IdM "dohraje" změny ze zdrojového systému, nebo naopak zkontroluje a sjednotí stav v cílovém systému (LDAP, AD apod.)," pokračuje pan Marek. Flexibilita Wren:IDM umožnila snadno implementovat i požadavky dané specifickým univerzitním prostředím, včetně přizpůsobeného uživatelského rozhraní.

Total Cost of Ownership

Univerzita v rámci výběru dodavatele kalkulovala pětileté celkové náklady zahrnující licenční poplatky, maintenance, podporu a opci na rozvojové práce v rozsahu až 1000 hodin. Podmínkou bylo předání kompletních konfigurací tak, aby nevznikla závislost na dodavateli. Kvůli tomu jsme také preferovali open-source platformu. Řešení od Orchitechu nabídlo transparentní cenovou politiku a univerzita nový systém získala za cenu jednoho roku licenční podpory předchozího řešení.

Ing. Jan Marek
Vedoucí Útvaru správy informační infrastruktury Jihočeské univerzity

řešení

Skartace osobních údajů

Správa identit je ze své podstaty vhodným nástrojem pro automatickou správu osobních údajů v řízených systémech, zejména často opomenutých procesů skartace, stanovených GDPR. Skartaci osobních údajů vyžaduje také ÚOOÚ.
V univerzitní praxi se ale objevují specifické výzvy. Může jít třeba o studenty nastupující na navazující studia nebo zaměstnance, kteří se vracejí pouze na jeden semestr. Okamžitá skartace by ovšem přinášela problémy při zachování kontinuity dat ve všech systémech organizace. Proto ji nejprve nahrazuje tzv. pseudonymizace. Ta sice smaže nepotřebné osobní údaje z identity, ale stále je možné provádět korelaci s využitím hashe unikátního identifikátoru identity. V takovém případě se identita obnoví díky načtení dat z personálních systémů. Až po uplynutí nastavené lhůty daného typu identity dochází ke skartaci, tedy ke kompletnímu smazání identity a navázaných vztahů.

Správa hostovských identit

Na veřejných vysokých školách je běžná velká fluktuace identit. Kromě studentů jde třeba o hosty konferencí a externí spolupracovníky, kteří potřebují vybrané přístupy jako WiFi a přístupové karty. Proto IdM umožňuje správu dočasných identit, resp. hostovských identit. Správu provádí administrátoři v rámci jednotlivých fakult, kde mohou pro každou fakultu definovat omezení – třeba maximální platnost či prefix uživatelského jména.

Celouniverzitní administrátoři mohou spravovat hostovské identity pro všechny fakulty. IdM se po založení hostovské identity postará o celý životní cyklus, přidělí všechny potřebné přístupy a ve správný čas zařídí jejich odebrání. Při zavádění nového řešení jsme se však museli potýkat i s chybami předchozího systému, které jsme se rozhodli jednou provždy nechat v minulosti.

Udržení kontinuity při opuštění univerzity

Uživatelé mohou využívat některých služeb i určitou dobu po opuštění univerzity – třeba přistupovat k univerzitní emailové schránce.

Toto jsme vyřešili zavedením konfigurovatelných karenčních lhůt. Lhůty jsou specifické pro různé typy identit a jejich parametry lze libovolně upravovat. Pro každou identitu je při jejím ukončení vypočítána doba uchování. Až po jejím uplynutí dojde ke skutečnému ukončení identity a zablokování přístupů. Na vypočítanou dobu uchování jsou navázány i další procesy, např. nastavení přesměrování pošty na osobní e-mail.

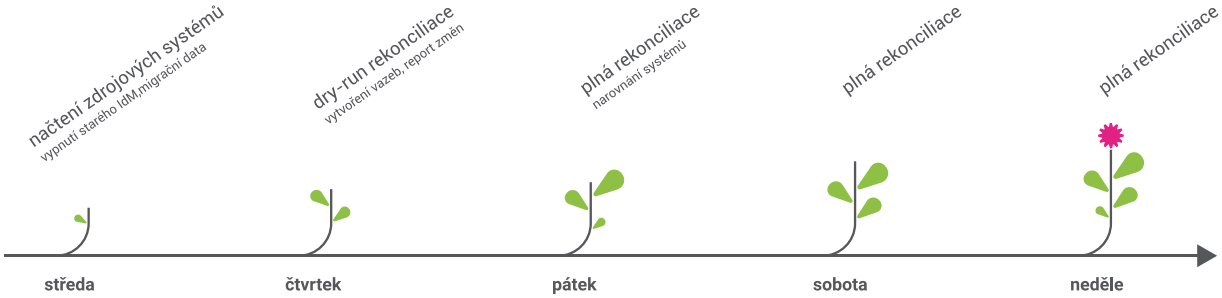
Problémy odhaleny již při implementaci

Při implementaci jsme s využitím synchronizace v režimu simulovaného zápisu („dry run“) objevili řadu problémů konzistence dat, které přetrvávaly z původní IdM:

- V Active Directory jsme odhalili řadu nekonzistencí v atributech (mezery za jménem, čárky v DN apod.).
- Konvence pro uživatelské jméno v některých případech generovaly jméno delší než 20 znaků, a docházelo tak k překročení limitu v AD (původní nahrazované IdM jméno bez chyby zkrátilo).
- Hesla obsahovala řadu neshod, neboť heslové politiky původního IdM nebyly sladěny s požadavky AD. Data v původním IdM tak nebyla v souladu s daty AD.
- Další nepřesnosti byly v e-mailových adresách vygenerovaných původním IdM, které neodpovídaly požadovanému algoritmu. Nové IdM tyto problémy napravivlo.
- LDAP pro FreeRADIUS obsahoval vícehodnotové záznamy v atributech, které měly být single-value. Původní IdM problém nehlásilo, a některé účty tak mohly být interpretovány mylně.
- Některé systémy vynucovaly referenční integritu, kterou IdM mělo zohlednit mj. správným pořadím zakládání a modifikace záznamů. Jelikož se toto nedělo, operace původního IdM mohly končit chybou a data nebyla řádně synchronizovaná.

Díky včasné identifikaci jsme tyto problémy vyřešili začištěním dat a úpravou IdM skriptů, a tak následný přechod do produkce proběhl hladce.

migrace



Díky pečlivé přípravě proběhla kompletní produkční migrace během necelého týdne. Přechod na nové IdM proběhl bez výpadku a bez dopadu na koncové uživatele.
Po přechodu dramaticky poklesla chybovost zpracování IdM procesů.

14 000	**33 000**	**80**	**8**
korektně napárovaných validních účtů	zakázaných účtů bez vlastníka (účty bývalých studentů)	nesprávně povolených účtů (účty, které měly být zakázány, ale nebyly)	chybějících účtů (účty, které dle IdM měly existovat, ale neexistovaly)

O Jihočeské univerzitě

Jihočeská univerzita v Českých Budějovicích patří mezi 10 největších univerzit v České republice. Navštěvuje ji více než 10 000 studentů, jejichž výuka zaměstnává stovky pracovníků.
Řízení přístupů k IS/IT je na JU náročné nejen kvůli počtu identit, ale i díky pravidelnému nárazovému příchodu a odchodu studentů v jednotlivých studijních obdobích.
S Orchitechem spolupracuje již od roku 2014.

Jihočeská univerzita
v Českých Budějovicích
University of South Bohemia
in České Budějovice

spolupráce

O nás

Pomáháme IT oddělením se správou identit a přístupů, což jim vyřeší jednu ze čtyř kritických komponent organizační bezpečnosti, přinese úsporu nákladů na správu identit, odstraní stres z auditu a IT se tak může soustředit na strategické business cíle.
S naší pomocí můžete efektivně spravovat a zabezpečovat identity zaměstnanců, externích pracovníků, studentů i zákazníků. Naše portfolio zahrnuje minimalistická řešení aktuálních problémů i robustní systémy zcela pokrývající procesy firmy.
V průběhu let jsme úspěšně dokončili více než 150 projektů pro přibližně 50 klientů a jsme hrdi na naše dlouhodobé vztahy s partnery, často trvající více než 10 let.

orchitech

https://orchi.tech/
+420 216 216 850
info@orchietch.cz